X Company Bilgi Teknolojileri Kabul Edilebilir Kullanım Politikası

Politika Adı	**Bilgi Teknolojileri Kabul Edilebilir Kullanım Politikası**
Politika ID	XCO-BT-POL-001
Sürüm	2.0
Yürürlülük Tarihi	18 Ekim 2025
Sorumlu Departman	Bilgi Teknolojileri (BT) Departmanı
Son Güncelleme Tarihi	18 Ekim 2025
Onaylayan	Yönetim Kurulu / CTO (Chief Technology Officer)

1. Amaç ve Kapsam

1.1. Amaç:

Bu politikanın amacı, X Company'nin bilgi teknolojileri altyapısının, yazılım geliştirme ortamlarının ve dijital hizmetlerinin **güvenli, yasal ve etik standartlara uygun** biçimde kullanılmasını sağlamaktır. Teknoloji odaklı bir organizasyon olarak, bilgi güvenliği, veri gizliliği ve sistem sürekliliği bizim için yalnızca bir zorunluluk değil; **inovasyonun sürdürülebilirliği için stratejik bir gerekliliktir.**

1.2. Kapsam:

Bu politika; X Company çatısı altında çalışan tüm **yazılım geliştiricileri, sistem yöneticileri, proje ekipleri, danışmanlar, stajyerler ve üçüncü taraf hizmet sağlayıcıları** için geçerlidir. Politika, şirketin sahip olduğu veya yönettiği tüm **donanım, yazılım, bulut servisleri, ağ altyapısı, veri merkezleri, IoT cihazları ve geliştirme ortamlarını** kapsar.

2. BT Destek ve Talep Yönetimi

X Company, çalışanların dijital verimliliğini artırmak amacıyla çok kanallı bir BT destek sistemi kullanmaktadır:

- **Kurumsal Asistan (AI Destekli Chatbot):**
  Şifre sıfırlama, yazılım lisans talepleri, VPN sorunları, erişim hataları ve diğer teknik işlemler için **birincil iletişim kanalıdır**. Asistan, talepleri analiz ederek otomatik yönlendirme veya anlık çözüm önerileri sunar.

- **BT Destek Portalı:**
  Yazılım kurulum talepleri, donanım arıza bildirimleri ve erişim yetkisi başvuruları için kullanılmalıdır. Her işlem, benzersiz bir **talep numarası (Ticket ID)** ile takip edilir.

- **Acil Müdahale Kanalı:**
  Kritik sistem kesintileri, veri ihlali, sunucu erişim kaybı veya üretim sistemlerinde duraksama gibi **iş sürekliliğini etkileyen durumlarda**, BT Olay Müdahale Ekibi'ne ulaşılmalıdır:
  📞 **+90 212 555 1234** | ✉ **incident@xcompany.com**

---

3. Kimlik Doğrulama ve Şifre Güvenliği

3.1. Güçlü Şifre Politikası:
Tüm kullanıcı hesapları, minimum **12 karakter** uzunluğunda; büyük/küçük harf, rakam ve özel karakter içeren şifrelerle korunmalıdır. Şifrelerde doğum tarihi, kullanıcı adı veya basit diziler kullanılmamalıdır.

3.2. MFA (Multi-Factor Authentication):
Kaynak kod depoları (Git, GitLab, Bitbucket), VPN erişimleri, e-posta sistemleri ve bulut yönetim panellerinde **MFA zorunludur.**

3.3. Şifre Yenileme Döngüsü:
Tüm kullanıcılar şifrelerini **her 90 günde bir** değiştirmelidir. Güvenlik denetimleri, bu süreyi aşan hesapları otomatik olarak kilitleyebilir.

3.4. Gizlilik ve Sorumluluk:
Şifreler veya API anahtarları hiçbir koşulda başkalarıyla paylaşılmamalıdır. Yetkisiz erişim şüphesi durumunda **Kurumsal Asistan** üzerinden derhal olay bildirimi yapılmalıdır.

---

4. Uzaktan Erişim (VPN & Bulut Güvenliği)

4.1. VPN Kullanımı:
Tüm uzaktan erişimler, BT Departmanı tarafından yapılandırılmış **kurumsal VPN altyapısı** üzerinden gerçekleştirilmelidir.
Kişisel VPN, proxy veya uzak masaüstü servisleri yasaktır.

4.2. Bulut Servisleri:
X Company tarafından onaylanmamış hiçbir bulut depolama servisi (örnek: kişisel Google Drive, Dropbox vb.) iş amaçlı kullanılmamalıdır.
Şirket, **Azure, AWS ve Google Cloud** üzerinde izlenen güvenli tenant'lar aracılığıyla çalışır.

4.3. Geliştirici Ortamları:
Kodu dışa aktarma, harici repository'ye paylaşma veya "public repo"ya aktarma sadece **bilgi güvenliği onayı** sonrasında yapılabilir.

---

5. Şirket Varlıklarının Kullanım İlkeleri

5.1. Kullanım Amacı:
Şirket tarafından sağlanan tüm cihazlar, yazılım geliştirme, test, analiz, proje yönetimi ve iş iletişimi gibi **kurumsal görevler** için tahsis edilmiştir.
Kısıtlı ölçüde kişisel kullanım, iş sürekliliğini veya güvenliği etkilemediği sürece kabul edilebilir.

5.2. Yasaklı Faaliyetler:

- Lisanssız veya crackli yazılım yüklemek,
- Oyun, torrent veya yasa dışı içerik sitelerine erişmek,
- Şirket ağı üzerinden kripto madenciliği yapmak,
- Şirket verilerini kişisel e-posta hesaplarında saklamak,
- Güvenlik duvarı, antivirüs veya sistem yapılandırmalarını izinsiz değiştirmek.

5.3. Cihaz Güvenliği:
Dizüstü bilgisayar, telefon veya geliştirici cihazlarının kaybolması veya çalınması durumunda, olay **en geç 2 saat içinde** yöneticinize ve BT Destek ekibine bildirilmelidir.

---

6. Yazılım Talep, Kurulum ve Lisans Yönetimi

6.1. Talep Süreci:
Yeni yazılım veya araç ihtiyacı olan çalışanlar, **Kurumsal Asistan** veya **BT Portalı** üzerinden "Yazılım Talep Formu" oluşturmalıdır.
Her talep;

- Güvenlik uyumluluğu,
- Lisans geçerliliği,
- Sistem entegrasyon etkisi
  açısından değerlendirilir.

6.2. Açık Kaynak Kullanımı:
Açık kaynak kütüphanelerinin projelerde kullanımı desteklenmektedir; ancak lisans türü (**MIT, GPL, Apache, BSD**) BT tarafından incelenmelidir.
GPL türevi lisanslar, kaynak paylaşım zorunluluğu doğurabileceğinden dikkatle kullanılmalıdır.

6.3. Güncellemeler:
Yazılımlar, en geç **her çeyrekte bir** güvenlik yamaları ile güncellenmelidir. Kritik açıklar tespit edildiğinde, güncellemeler zorunlu olarak uygulanır.

---

7. Siber Güvenlik Farkındalığı ve Bildirim Yükümlülüğü

7.1. Farkındalık Programı:
Tüm çalışanlar, yılda en az bir kez **"Siber Güvenlik Farkındalık Eğitimi"** almakla yükümlüdür.
Yeni başlayanlar, oryantasyon sürecinde temel BT güvenlik eğitimini tamamlamalıdır.

7.2. Şüpheli Durum Bildirimi:

- Bilinmeyen gönderenlerden gelen e-postalar,
- Kötü niyetli bağlantılar veya ek dosyalar,
- Şirket içi olmayan oturum açma denemeleri,
  gibi olaylar tespit edildiğinde **guvenlik@xcompany.com** adresine yönlendirilmelidir.

7.3. Olay Müdahalesi:
BT Güvenlik Ekibi, olayları **CIRT (Computer Incident Response Team)** prosedürlerine göre değerlendirir. Kullanıcı, olay incelemesi süresince BT ile iş birliği yapmakla yükümlüdür.

---

8. Politika İhlalleri ve Disiplin Süreci

Politika ihlalleri, X Company'nin dijital güvenlik standartlarını tehlikeye atabileceğinden ciddi sonuçlar doğurur.
Olası yaptırımlar:

- Yazılı uyarı,
- Sistem erişimlerinin askıya alınması,
- Disiplin cezası,
- Gerekirse iş akdinin feshi.

Yasal ihlal durumlarında, olay ilgili **siber suç birimleri** ile paylaşılabilir.

---

9. Politika Gözden Geçirme ve Güncelleme

BT Departmanı bu politikayı **her yılın son çeyreğinde** gözden geçirir.
Yeni teknolojik gelişmeler (örneğin yapay zekâ araçları, kod üretim sistemleri, bulut mimarileri) doğrultusunda gerekli revizyonlar yapılır.
Politikanın güncel sürümü **intranet portalı** üzerinden yayımlanır.

---

10. Onay ve Uygulama

Bu politika, **X Company Yönetim Kurulu** tarafından onaylanmış olup, **18 Ekim 2025** tarihinden itibaren yürürlüktedir.
Tüm çalışanlar, işe girişte bu politikayı okuduklarını ve kabul ettiklerini yazılı olarak beyan ederler.

🛡 **“Güvenlik, inovasyonun temelidir.”**

X Company, teknoloji üretirken bilgi güvenliğini kültürünün bir parçası haline getirmeyi taahhüt eder.